www.seetconf.futminna.edu.ng

www.futminna.edu.ng

A PACKET SAMPLING THRESHOLD TECHNIQUE FOR MITIGATING DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS IN A UNIVERSITY CAMPUS NETWORK

B. Dominic[1*], H.C. Inyiama[2], A. Ahmed[3], M. B. Abdullahi[4] and O. M. Olaniyi[5]
[1,2,4]Computer Science, Federal University of Technology, Minna
[3,5]Computer Engineering, Federal University of Technology, Minna
aliyu.ahmed@futminna.edu.ng, 07068234414.

ABSTRACT
Over the years, the Distributed Denial of Service (DDoS) attacks have evolved from simple flooding attacks to more complex attacks. With the advent of e-examination and online registration, higher institutions of learning may be exposed to online attacks such as DDoS attacks especially at the application layer.In this paper, a mitigation technique known as Packet Sampling Threshold (PST) technique is developed on a modeled logical Campus network to prevent DDoS attacks on the servers at the application layer. The results obtained from the simulation in OPNET modeler 14.5 showed that the technique was effective and efficient in securing the Campus network against the DDoS attacks.

Keywords:*Packet sampling threshold, distributed denial of service attacks, campus network*

1. INTRODUCTION

Over time, Distributed Denial of Service (DDoS) attacks have grown from simple flooding attacks to more complex attacks. As such, any organization that uses the Internet is vulnerable to attacks online. Nonetheless, the educational sector is also subjected to DDoS attacks following the emergence of school e-examination and online registration. DDoS attackers have modified their attack methods in a pattern that is now more difficult to detect, thereby dimming the line between attacking source and legitimate users (Juniper, 2008).

According to Wesam and Mehdi (2014), DDoS attacks usually overshadow network resources with useless or harmful packets that can prevent legitimate users from gaining access to these resources thereby, infringing on the confidentiality, privacy and integrity of information on the network.

A Campus is a main enterprise location which is made up of one or more buildings that are in close proximity. Usually, a Campus is not necessarily the corporate head-quartersor a major site but rather, it is a multi-floor office building that houses an enterprise, a university or a corporation made up of several buildings in an office complex and the set of interconnected local area networks (LANs) serving the enterprise or the university is referred to a Campus Network (Juniper, 2010). In a Campus Network, all the buildings and floors on the Campus are being connected together in order to share resources and services in a data center either through a campus Local Area Network (LAN) or Wide Area Network (WAN) connections. The Campus could also be connected to remote locations such as branch or regional offices through a WAN (Juniper, 2010).

In today's modern and global world that is Information Technology driven, the necessity and increase values provided by network infrastructures have shown its importance in government organizations, business enterprises and educational institutions most essentially Universities. This has contributed greatly to the achievement of some important goals such as increased productivity, partnership, efficiency and acquiring of knowledge in frequent researches for educational purposes. Therefore, to increase the use of Information Technology in higher institutions of learning requires a robust technical

infrastructure to provide for a secured and reliable network. A University Campus Network is a great necessity for knowledge sharing, easycommunication and aids in collaborative research which are the essential ingredient to building a strong knowledge culture and efficiently support academic mission.

The reminder of this paper is structured as follows: Section 2 presents the review of related works, Section 3 discusses the methodology used in the research and Section 4 presents the Results and discussion while the Conclusion is given in Section 5.

2. REVIEW OF RELATED WORKS

Anjali and Padmavathi (2014) proposed a novel method of detection of DDoS attacks based on Chaos theory and Artificial Neural Networks. The proposed detection technique based on Chaos theory effectively detects DDoS attacks but there is possibility of large prediction error due to busty network traffic.Shalaka, Madhulika, Prajyoti, Sneha and Nilesh (2014) proposed an architecture known as Secure Overlay Services (SOS) to proactively prevent denial of service attacks. Probability of successful attack was reduced by performing intensive filtering near protected network edges, pushing the attack point into the core of the network where high speed routers can handle volume of attack traffic and by introducing randomness and anonymity into the forwarding architecture making it difficult for an attacker to target nodes along the path to a specific SOS protected destination.

Shalaka *et.al*.(2014) used a simple analytical model to evaluate the likelihood that an attacker can successfully launch a DoS attack against an SOS protected network. The result of the proposed SOS architecture showed the resistance of a SOS network against DoS attack as the number of nodes that participate in the overlay increases but the method is limited to classes of communication where the attackers are known.

The Study of Deepak, Puneet and Vineet (2014) focused on the behaviour of a server or victim machine with regards to various parameters (traffic drop, CPU Utilization, TCP retransmission count, memory free size and processing delay) under DDoS attack using a LAN network simulated in OPNET modeler. A study on prevention strategies and network intrusion prevention techniques for DoS attacks was carried out by Arshey and Balakrishnan (2013). The detection and prevention techniques discussed show that it is effective for small network topologies and can also be adapted for large domains. Arshey and Balakrishnan (2013) reported on some DoS attack mechanisms, how they operate and suggested some basic mitigation strategies that can be adopted to prevent these attacks.

Kharat and Radhakrishna (2013) in their study proposed a threshold based approach technique to detect and prevent DDoS attack before it reaches the victim end with high detection rate and low false positive rate to achieve high performance. Hak (2013) in his study, present DoS attacks and explore several methods of combating these attacks, he describe and analyze the techniques used to detect, prevent and mitigate these DoS attacks.Aamir and Arif (2013) further provided a simulation based analysis of an FTP server performance in a typical enterprise network under DDoS attack. The simulation done in OPNET showed noticeable variations in connection capacity, task processing and delay parameters of the attacked server as compared to the performance without the attack.Lonea, Popescu and Tianfield (2013) proposed a solution using Dempster Shafter Theory (DST) operations in three-valued logic and the Fault-Tree Analysis (FTA) for each virtual machine-based Intrusion Detection System (IDS) in

order to reduce false alarm rates by the representation of the ignorance.

3. METHODOLOGY

Figure3.1 shows the steps that are followed to develop and simulate the Campus Network. It is assumed that the management information system (MIS) unit is responsible for the management of the campus network and thus, houses the core of the network facilities. The design and simulation of the network was carried out in OPNET modeler.

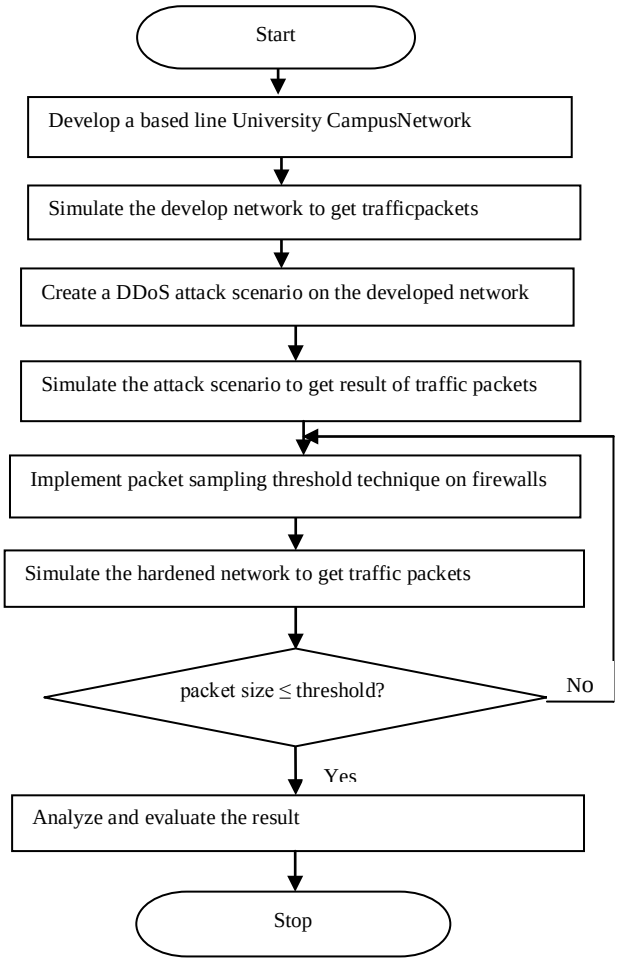

Fig. 3.1: Flow Chart for the Development and Simulation of the Campus Core Network

3.1. Modelling of the Campus Core Network

The Campus Core Network was modelled in OPNET modeler 14.5. The model of the real system was done in three scenarios, namely: the baseline busy scenario, the attack scenario and hardened scenario.

3.1.1. Baseline Busy Model

The baseline scenario was configured adopting the Campus Core Network which served as the baseline scenario busy network in which normal traffic packets were injected into the network and was configured to run under normal circumstances assumed for the normal traffic packets.

The parameters considered for the design of the baseline busy scenario is computed using equations 1 and 2.

$$Tr = \sum_{i=1}^{n} y_i \quad (1)$$

$$Ta = \sum \frac{y_i}{N_i} \quad (2)$$

Where T_r and T_a are Traffic and average traffic respectively, and y = values of packet traffic on the network and $i = 1, 2, 3 \ldots n$. Also the Normal traffic, Nt is calculated using equation 3 assuming a baseline busy traffic of 99% generated.

Thus;

$$Nt = 0.99Tr \quad (3)$$

The baseline busy scenario model is shown Figure 3.2, representing the MIS (Management Information System) subnet that houses the FTP server, Web server sand VoIP server. It also shows the core switch

that connects the MIS subnet to other subnets in the network.

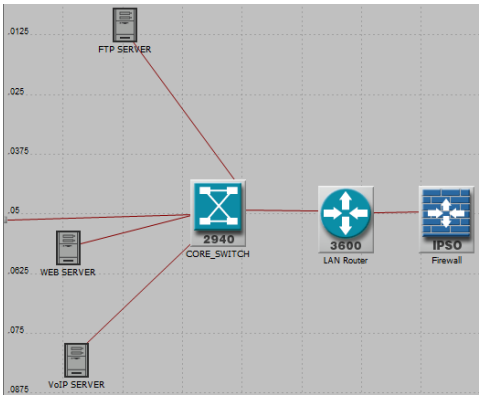

Fig. 3.2: MIS Core subnets for the Baseline Scenario showing the servers

3.1.2. The Attack Model

It is assumed that the attackers got control of the botnets consisting of the zombies and handlers and succeeded to pass through the firewall of the network. A DDoS attack scenario is configured and attack traffic packets are injected into the developed network.10 LAN workstations configured in promiscuous modes served as the botnets consisting of the zombies and the handlers. Botnet 1 is the attacker 1 attacking the FTP server, botnet 2 is the attacker 2 attacking the web (HTTP) server, while botnet 3 is the attacker 3 attacking the VoIP server. Attackers 1 and 2 are operating from remote sites (see Figure 3.3) while attacker 2 is attacking from within (see Figure 3.4). The attacker 1 floods the FTP server with large traffic packets above the assumed normal packets that can be handled by the FTP server; attacker 2 also floods the web server with large request above the normal request packets the web server can handle and attacker 3 also floods the VoIP server with large request above normal thereby affecting the normal performance level of the servers.

For Attack Traffic, A_t,with assumption value of 300% traffic scaling for 10 workstations that make up the zombies and handlers, the derived attack traffic is given in equation 4.

$$A_t = 30Tr \quad (4)$$

The Attack Scenario model is shown in Figure. 3.3 and 3.4.

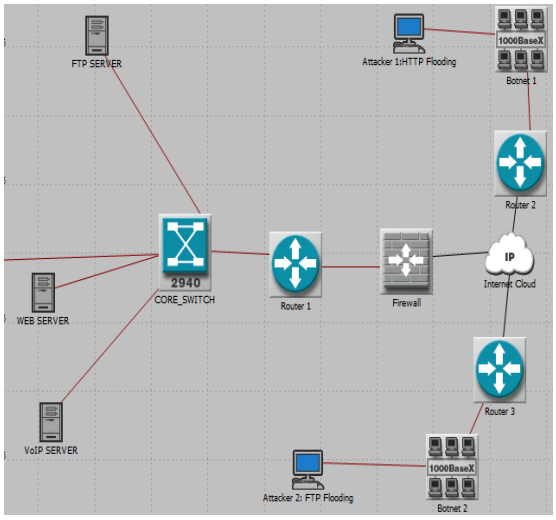

Fig. 3.3: Attack scenario showing attackers from remote sites on the FTP and Web Servers

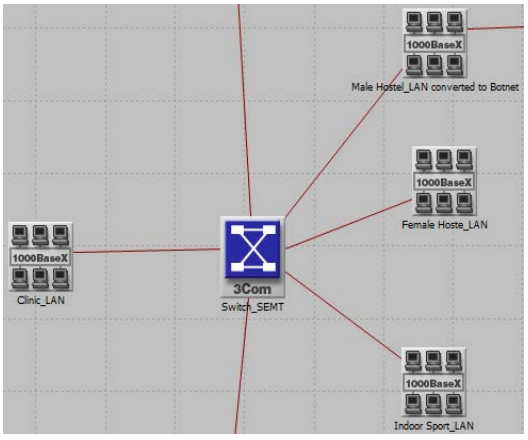

Fig. 3.4: The attack scenario of the VoIP server from within the MIS network.

3.1.3. Hardened Network Model

In the modelling of the hardened scenario security is implemented against the DDoS attacks, Packet Sampling Technique (PST) is applied on two separate firewalls on the simulated network, one for inbound traffic and the other for outbound traffic. In the technique, a threshold is set such that once any incoming traffic packet is greater than the set threshold; such a packet is labelled as an attack packet and hence discarded. Therefore, the first firewall is located in the MIS core network at the subnet before the MIS core Switch to secure against attacks from within the network.The second firewall securing against attack from remote sites that is, outbound traffic attack is located between the Internet Service Provider (ISP) and the Router connecting to MIS core servers as shown in Figure3.5.

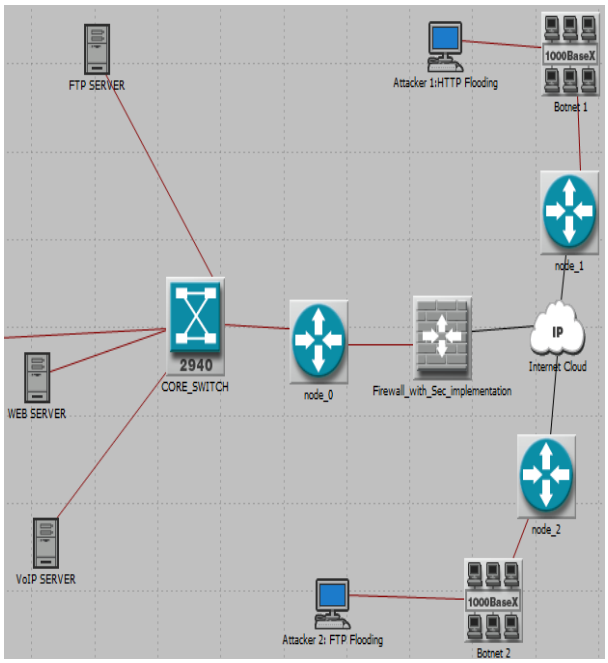

Fig. 3.5: Firewall configured between the ISP and Router before the MIS Core Switch

The implemented PST algorithm is shown Figure3.6.

1: Classify traffic flow using packet sampling
2: Measure traffic flow (T_x) in packet/second
3: Calculate the average traffic (T_a)
4: Compare each traffic flow with average traffic
5: If $T_x > T_a$
6: Mark packet as an attack packet and discard
7: Else,
8: Allow legitimate traffic packet to be delivered.

Fig.3.6: PST algorithm

3.1.4. PST Mechanism

Packet Sampling Scheme detects DDoS attack flows on huge networks by considering measures of flow entropy, average entropy, the entropy of the source port and the number of packets/seconds. It looks at the incoming traffic and extract at an average random, one data packet for sampling during a time window specified by the algorithm. The packet is forwarded or discarded based on the entropy value as compared to the threshold value set. The process is depicted in Figure 3.7.

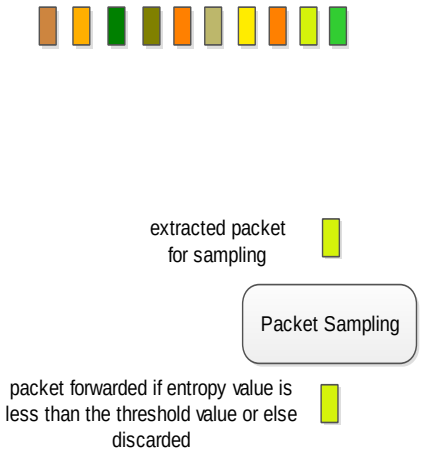

Fig. 3.7: Packet Sampling implemented on router

4. RESULTS AND DISCUSSIONS

Server side parameters such as CPU Utilization, Load response time and Delay are considered to analyse the

effect of the DDoS attack on the performance of the servers in the simulated network.

4.1. Comparison of the Results from the Attack and Hardened Scenarios

It can be seen from the graph in Figure 4.1 that the Web (HTTP) server utilization during the attack scenario is very high, getting to the peak value of 0.28 percent CPU utilization because more traffic packets is being sent by the attacker to the server in order to exhaust the server by requiring more of its processing time. However, the result shows that the web server utilization under the Hardened Network is reduced with initial rise to the peak value of about 0.08 percent and then drastically reduced to almost 0.02 percent CPU Utilization. This indicates that the server was less utilized in the Hardened network scenario as a result of PST that was implemented to help in filtering off the abnormal or flooded traffic thereby maintaining normal CPU utilization and preventing the DDoS attack on the Web server.

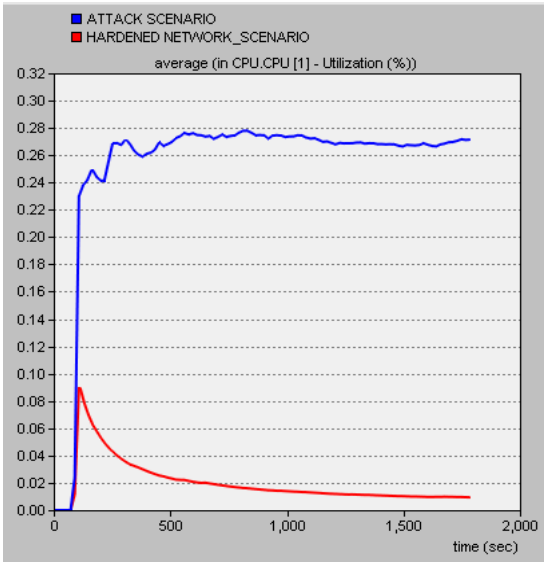

Fig.4.1: Web Server – CPU Utilization (%)

Figure 4.2 shows that under the attack scenario there is a peak rise of email load in sessions per seconds as compared to the result of a low email load under the hardened scenario. In the first instance, because of the over flooding of the web server, more session are requested leading to the rise in load session per seconds while in the hardened scenario, the attack traffic have been filtered thereby reducing the email load on the web server. This shows that the PST was able to block and prevent further attack on the web server.

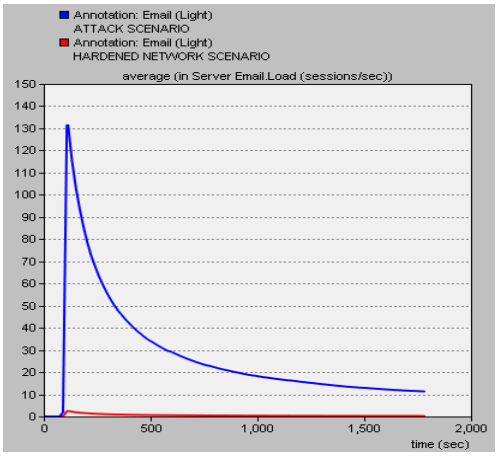

Fig. 4.2: Web Server – Load (Sessions/Sec)

From the graph in Figure 4.3, the result of the VoIP server for the voice called party jitter measured in seconds shows that there is a rise to 600 microseconds for the attack scenario. The attacker floods the server with more traffic packets to exhaust the server. This makes server to be busy processing these packets preventing it to attend to the legitimate requests. However, in the hardened scenario the packets jitter dropped to about 1.6 microseconds. This result has shown that the implemented PST is able to secure the VoIP server from over flooding with the attacker's illegitimate and unnecessary traffic packets.

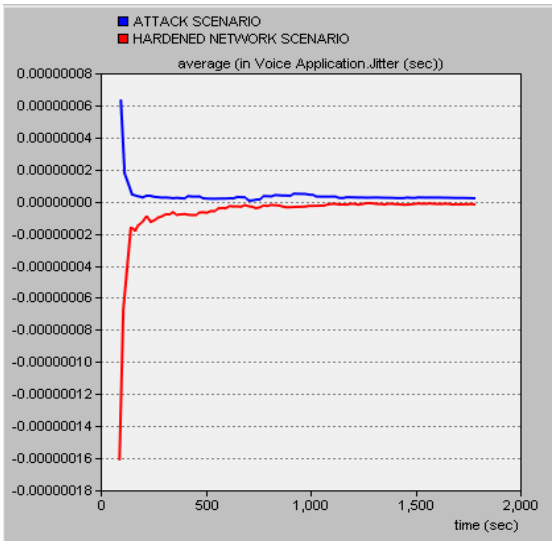

Fig.4.3: VoIP server – Jitter (seconds)

Also, it can be observed from Figure 4.4 that, in the Attack Scenario the load on the FTP server is high to about 0.64 load(requests per seconds) because of the flooding of the server with more requests by the attacker and consequently increasing the connection requests time. However, in the Hardened scenario, the load on the FTP server dropped drastically, which shows that the PST mitigation technique implemented effectively secured the server from the attacker's unnecessary flooding requests.

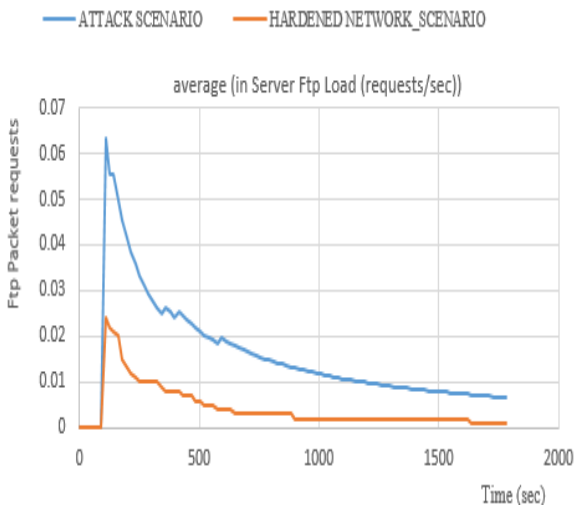

Fig. 4.4: FTP server – Load (request/sec)

5. CONCLUSION

In this paper, Packet Sampling Threshold (PST) technique was implemented on two separate firewalls in a modelled Campus Core Network to mitigate Distributed Denial of Service (DDoS) attack. In the technique, a threshold was set such that once any incoming traffic packet is greater than the set threshold; such a packet is labelled as an attack packet and hence discarded.The results from the simulation carried out on OPNET Modeler 14.5 showed that the PST technique implemented was able to block the DDoS attacks on the servers. In this way, the system load is greatly reduced and DDoS attacks were prevented in real time.

Furthermore, hybrid techniques can be adopted such as the combination of the Packet Sampling Technique (PST) with neural network to improve the effectiveness of the security of a Campus Network against DDoS attacks.

REFERENCES

Anjali, M. & Padmavathi, B. (2014). DDoS Attack Detection Based on Chaos Theory and Artificial Neural Network. *Journal of Computer Science and Information Technologies*, 5(6), 7276-7279.

Arshey, M. & Balakrishnan, C. (2013). Prevention Strategies and Network Intrusion Prevention Techniques for DoS Attacks. *International Journal of Advanced Research in Computer Engineering*, 2 (2),1174-1178.

Deepak, A., Puneet, S. & Vineet, S. (2014). Impact Analysis of Denial of Service (DoS) Due to Packet Flooding. *International Journal of Engineering Research and Applications*, 4 (6),144-149.

Hak, J. K. (2013). An Introspective view of Denial of Service (DoS): Detection, Prevention and Mitigation.

International Journal of Scientific Knowledge, 3 (40),10-15.

Juniper, (2008). Protecting the Network from Denial of Service Floods. Available athttp://www.juniper.net. Retrieved on 01-06-2008. 1-10.

Juniper, (2010). Design Considerations for the High-Performance Campus LAN. Available at http://www.juniper.net. Retrieved on 10-06-2010.

Kharat, J.S. & Radhakrishna, N. (2013). A Vivacious Approach to Detect and Prevent DDoS Attack. *InternationalJournal of Research in Engineering and Technology*, 2 (10), 434-440.

Lonea, A. M., Popescu, D. E. & Tianfield, H. (2013). Detecting DDoS Attacks in Cloud Computing Environment. *International Journal of Communication*, 8 (1), 70-78.

Shalaka, S. C., Madhulika, S. M., Prajyoti, P. S., Sneha, S. P. & Nilesh, S. (2014). Mitigating Denial of Service Attacks using Secure Service OverlayModel. *International Journal of Engineering Trends and Technology*, 8 (9), 479-483.

Wesam, B. & Mehdi, E. M. (2014). Review Clustering Mechanisms of Distributed Denial of Service Attack. *International Journal of Computer Science*, 10 (10), 2037- 2046.